2012

Feral Practices

Shubhankar Thatte
Swinburne University of Technology, sthatte@swin.edu.au

Nick Grainger
Swinburne University of Technology, ngrainger@swin.edu.au

Judy McKay
Swinburne University of Technology, jmckay@swin.edu.au

Feral Practices

Shubhankar Thatte
Nick Grainger
Judy McKay
Faculty of Information and Communication Technologies
Swinburne University of Technology
Melbourne, Victoria
Email:
sthatte@swin.edu.au
ngrainger@swin.edu.au
jmckay@swin.edu.au

Abstract

In this paper we introduce the concept of feral practices which we define as the usage of information technology which deviates from the standard organizational norms and which exists beyond the control and/or knowledge of the organizational IT management. We argue towards using a 'practice' perspective in understanding non-compliant IT practices where we suggest a greater emphasis on usage of IT artifacts rather than the artifacts itself. We also outline a scope of feral practices by clarifying some of the concepts associated with the phenomenon. We propose a model based on the Merton's Theory of Anomie, which seeks to explain why feral practices come about and what are the technological and social influences and supporting factors which lead to this phenomenon. This study thus intends to build a conceptual base for future studies on feral practices by providing a holistic view on the phenomenon and also identify directions for future research.

Keywords: Feral Practices, Feral Systems, Shadow Systems, Merton's Theory of Anomie, Deviance

INTRODUCTION

Billy Blogs, a sales executive in HappySales, always carries his company's iPad with him during his client meetings. He uses an online app to take orders from customers. The catch is that this application has not been sanctioned for use by the corporate IT department, who has laid down strict policies in terms of what software applications employees are allowed to use in the organization. What is more, the company Billy works for employs around ten sales professionals who use various different apps to take customer orders. The data gathered by each is not shared across the sales team and resides on everyone's own personal storage space. The company currently struggles to generate accurate numbers for the total orders that are being placed and hence struggles to meet the deadlines on time. In a different part of the world, Yosemite Sam, a project manager in TronixSoft, struggling to maintain collaboration and coordination in his team of twenty engineers with the available IT resources supplied by the company, decides to sign them up onto Flowdock, a cloud-based group communication tool. This nifty tool enables the engineers to share technical/functional documents and design outlines and create discussion groups to share technical knowledge and best practices and also keeps the team informed of any major project level changes by sending instant notifications. The team benefits immensely and delivers a large project on time. While Yosemite's team continues to derive benefits from the tool, the rest of the organization is oblivious of the tool and the benefits offered by it. But the CIO of TronixSoft is particularly concerned with the security and confidentiality of the data that is being put onto these cloud based applications and has a policy against employees storing organization data outside the company's firewall.

Both the examples described above, though seemingly different, share two common themes. Firstly, both the practices, while innovative and of benefit to individuals and groups, are actually having negative impacts on the organization, and would most likely be breaking or deviating from organizational norms with regards to acceptable IT usage. Secondly, these practices could be seen as being conducted outside the knowledge and/or control of organizational IT management. In the first example, there seems to be a clear issue with respect to data integration as data is being stored in disparate locations. Also there might be an issue regarding the maintenance of confidentiality of customer and organizational data as the applications being used might not have adequate security safeguards. While in the second example, very crucial organizational documents are being stored on a public website, which might not only have issues in terms confidentiality of organizational data but also in terms of protecting the intellectual property (IP) of the organization. Moreover the benefits

gained from the tool are being restricted to a specific part of the organization and are not being shared with the rest who could potentially benefit from the collaborating capabilities of the tool. These types of end-user IT practices are what we call *Feral Practices,* which can be defined as the usage of information technology that deviates from the standard organizational norms and which exists beyond the control and/or knowledge of the organizational IT management.

Feral practices are certainly not new to the organizational IT landscape. From the early years of personal computers and user-friendly productivity tools (such as Microsoft Excel, Word) to the latest technology paradigm (which includes mobile computing, cloud computing, web 2.0, etc), studies have shown that end users seem to have found ways to circumvent organizational IT policies and procedures (King 2012; Markus 1983). But with IT becoming more pervasive, user friendly, consumer-oriented and relatively cheap, there seems to have been a greater surge in these practices in organizations. According to the latest study by Gartner as quoted by King (2012), in the next three years, '35% of the enterprise IT expenditures will happen outside of the corporate IT budget' while King (2012) citing a study by PricewaterhouseCoopers (PwC), has suggested that in the 100 top-performing companies, IT controlled less than 50% of the corporate IT expenditures. These statistics seem to suggest that business units and end-users are increasingly gaining control over their own IT needs by deciding what applications they want, and either buying the required software or building their own. This might further suggest that feral practices will continue to gain ground in organizations as control seems to have shifted from the corporate IT department to end-users who now appear to be demanding more control over the applications and devices they want to use in their routine work. But on the other hand the IT department is still seen as the unit that has a responsibility to ensure that none of these end-user initiatives pose any harm to the organization. As organizations struggle to find ways to effectively manage feral practices it is imperative that the IT management understand why these practices originate and what technology and social influences drive some of the feral practices, in order that they can then establish better policies and management strategies.

The objective of this paper is thus to firstly introduce the concept of feral practices, to subsequently develop a framework which explains why feral practices originate, and what are some of the technological as well as social influences which promote this phenomenon. This paper makes a significant theoretical and practical contribution. Theoretically, this study takes a 'practice' view of the end user feral initiatives (as discussed in the above examples) as compared to current studies that focus primarily on the systems that result from feral practices. This study thus intends to provide a new perspective on the non-compliant IT behaviors of end users and thus provides relevant arguments to support the practice view taken in this paper. This paper also integrates the technological and social influences provided by the previous studies into a single framework which provides insights into why feral practices come about and how these influences play a part in promoting the non-compliant behavior. None of the existing studies have taken such a comprehensive view on feral practices. The practical contribution of this paper is derived from the generation of greater understanding of a ubiquitous, but seemingly un-discussed and under-researched phenomenon. We thus see that this paper makes a significant contribution as it sets out a clear direction for future research by clarifying important concepts related to these practices and identifying areas which could be explored in the future, thus resulting in building theoretical and practical knowledge in this domain.

This paper is structured as follows: in the next section we briefly discuss feral practices and explain certain concepts associated with these practices. We then explore the technological and social influences behind feral practices by using Merton's theory of Anomie (1938). In the final section we identify future directions and potential contributions of this research.

FERAL PRACTICES – DEFINITION

Feral practices can be broadly defined as usage of information technology which deviates from organizational norms and exists beyond the control and/or knowledge of the organizational IT management. In the definition, *norms* are defined as the "boundaries between prescribed and proscribed behaviors in a particular institutional setting" (Dubin 1959, p149) which delineate the "range of what people subject to the particular institution are normatively expected to believe and to do" (Merton 1959, p178). Cloward and Ohlin (1960, p236) further suggest that the purpose of norms is to "delineate boundaries between legitimate and illegitimate practices". *Control* here is defined as the process, through which organizational management influences the behavior and output of the employees through mechanisms such as authority, social structure, technology and culture (Finnegan and Longaigh 2002; Orlikowski 1991). Feral practices thus can be tagged as illegitimate practices which thrive in organizational units where few controls and restraints exist to regulate them.

The adjective feral comes from the term *Feral Systems* (Behrens 2009; Kerr and Houghton 2008; Kerr et al. 2007) which are information systems that are not a part of the accepted information technology infrastructure and that are designed to circumvent official information systems and 'systemic' procedures (Kerr and Houghton

2008, p484). Feral systems have also been referred to as "Shadow Systems" (Behrens 2009; Behrens and Sedera 2004) or "Shadow IT" (King 2012) and "Workaround Systems" (Behrens 2009). While there might be subtle differences in the definitions of these terms, a characteristic shared by these definitions is that they are designed to circumvent the official systems and organizational procedures.

In this study we prefer to use the term Feral Practices rather than Feral Systems. Reckwitz (2002, p250) defines practices as routinized or patterned behaviors not only comprising of bodily activities but also mental activities of "understanding, knowing how and desiring". Practices are thus said to involve use of objects in specific ways (Reckwitz 2002). We intend to make a conceptual shift to feral practices because, firstly we perceive *ferality* is more specifically associated with the usage of the information system rather than the system and the feral system is seen as an outcome of the feral practice i.e. the system acquires feral properties due to the way it is designed and used. Thus feral practices not only involve the information system but also the specific usage of the system thereby enabling us to take a broader perspective on these non-compliant IT behaviors. Secondly taking a practice perspective, not only allows us to study information systems that reside outside the organizational IT infrastructure but also systems which are part of the infrastructure but which are used in a feral manner. This is specifically important in the context of the latest technological landscape involving consumerization of IT, BYOD, as the boundaries between an official and unofficial systems (or between systems residing within and outside the organizational IT infrastructure) have become blurred and the focus has mostly shifted towards regulating the usage of the IT artifacts by the end users to prevent violation of organizational norms. Finally, as evident from the definition of the term *practice*, the practice perspective not only provides us with an appropriate lens to analyze specific usage behaviors but also to understand the perceptions of the end-users who engage in those behaviors and account for the social contextual influences behind them (Orlikowski 2000; Reckwitz 2002; Schatzki 2000). A similar line of thought has been adopted by studies on workarounds where the focus is more on the specific usage of technology rather than the technological artifacts (Azad and King 2008; Azad and King 2011; Ferneley and Sobreperez 2006; Kobayashi et al. 2005; Koopman and Hoffman 2003).

FERAL PRACTICES – SCOPE

In the previous section we offered a fairly broad definition of feral practices. There is a tendency to regard these practices as negative, malicious, and thus potentially damaging to the organization. However, it is also important to consider whether these practices can be considered innovative, whether feral practices offer any benefits to an organization, and further, the status of the norms they are seen as violating. It currently appears very few studies have explicitly tried to answer these questions with regards to these non-compliant IT practices. Hence it appears that the scope of these practices is not very clear as presented in these studies. In this section we thus intend to define the scope of feral practices by attempting to answer these questions so as to develop greater clarity on these practices.

The concept of 'reference group' is important to understanding norms, as it is used to refer to the social group to which the norms apply (Warren 2003). It appears that there are two levels of reference groups that previous studies seem to suggest: firstly, the overall organizational management responsible for developing organizational-level norms regarding the general conduct of employees specifically related to the usage of IT in organizations, and secondly, the department or work group that is responsible for developing specific work related norms specific to the department or work group. Organizational level norms might be said to set expectations regarding issues such as data security, privacy, conduct regarding ethical use of social media etc while departmental or work-group level norms might be said to set the expectations regarding the roles and responsibilities of employees in the specific workgroup and specific workflows that need to be followed for conducting those roles and responsibilities involving the use of IT. Practices regarding IT can then be classified in a 2x2 matrix according to whether or not they follow or deviate from norms at either the organizational or work group level (see Figure 1 below). IT use can either comply at both levels (see (1) in Figure 1 below), or fail to comply with one or both sets of norms. Feral practices can thus be said to fall into three quadrants (2, 3, 4). In the case of (2) in Figure 1, practices follow work related norms but deviate from organizational norms. Behrens (2009) gives an example where academic staff of a university developed a system to circumvent the official system implemented by the higher organizational management. This system was considered feral by the organizational management and corporate IT as it contravened organizational rules and policies, but was considered essential for conducting routine tasks for the academic staff of the organization. In (3), practices follow organizational norms but deviate from the work related norms. For instance, consider a case where financial accountants store budget and forecast data in an excel spreadsheet rather than entering it into the corporate financial system**.** While organization management may not have any reservations about storing the data in the excel format, the finance department mandates the storage of the data in the finance system for reporting purposes**.** Thus this practice might be seen to be complying with the organizational norms but

violating the work related norms of the department. Finally in (4), are practices that deviate from both organizational and work-related norms. Markus (1983), in her study, shows how divisional accountants sabotaged a Financial Information System (FIS) in order to compete for power with the corporate accountants. By sabotaging the system, the divisional accountants not only tried to undermine the organizational policies but also tried to undermine the formal responsibilities of the organizational accountants.

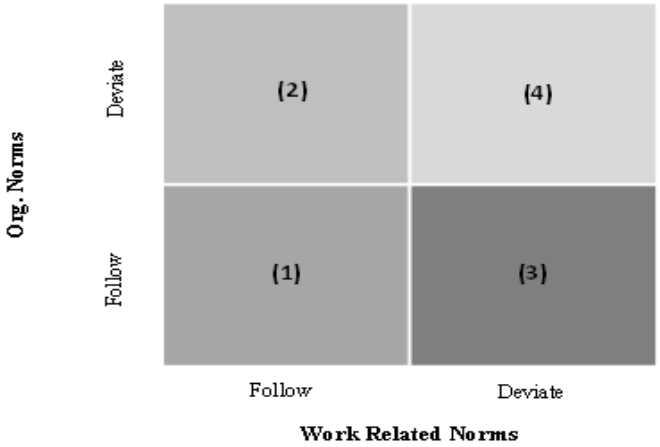

Fig 1. 2x2 Org Norms-Work Related Norm Matrix

While the tendency may be to regard feral practices in a negative light, it could also be asked if they are a source of innovation. Studies on innovation seem to suggest that practices can be considered innovative only if there is an element of newness in them for the adopting unit (a person, group, department or an organization) (Damanpour 1991; Downs and Mohr 1976; Downs and Mohr 1979; Slappendel 1996). We perceive that all feral practices may not be conceived as innovative i.e. despite the fact the behavior involved deviates from the norm, there might not be any element of newness in it for the adopting unit. For instance end-users developing parallel systems which replicate the functionality of a formal system cannot be seen as innovative as it may not be offering anything new to the adopting unit. But even if a feral practice is perceived as innovative by an adopting unit it might not be perceived to be so by the reference group (in the situation where the reference group and adopting unit are separate entities).

Furthermore with regards to whether feral practices are beneficial to an organization, current studies seem to have highlighted both the benefits and risks associated with feral practices. On one hand studies by Behrens and Sedera (2004); Kerr et al. (2007), have pointed to the risks that some of feral initiatives hold for an organization in terms of issues relating to data redundancy, data integrity, confidentiality etc. On the other hand studies by Behrens (2009), Ferneley and Sobreperez (2006); King (2012) have suggested that some of the feral practices are essential and potentially beneficial for the organization's interests. Furthermore, feral practices classified as innovative could be further classified as beneficial or potentially risky as well. For instance Yosemite Sam's initiative of setting up a way of enhancing collaboration within the team can be considered as innovative as well as beneficial from the work group perspective as not only was he able to devise a new way of achieving collaboration but was also able to lead the project to a successful completion. But at the same time adopting more of an organizational perspective, Sam's initiative could be seen as potentially risky as there is a potential threat to the intellectual property of the company being stolen as the sensitive data is being stored outside the company's firewall. The element of risk and threat thus brings to the fore the issue of whether certain feral practices may be regarded as malicious. We suggest that feral practices may or may not be malicious (i.e. conducted with the deliberate intent to cause harm to the organization or group or specific individual), but for our research we do not intend to include any malicious acts in the scope of feral practices. Thus feral practices might be seen as acts that deviate from the norms of organization (overall organizational management or work group) which are possibly innovative or creative but not malicious.

CONDITIONS FOR FERAL PRACTICES

Previous studies on feral systems have proposed several technological and social influences to account for deviance from overall organizational management or work group norms. In this section we argue that the structure of an organization exerts an overarching influence on deviance in feral practices through several technological and social influences as suggested by previous studies exploring non-compliant IT practices. To demonstrate this we use the Theory of Anomie proposed by Merton (1938) that has suggested how social structure promotes deviance in certain societies leading to a state of normlessness or 'social disequilibrium'

where the rules governing human conduct have lost their 'savor or force' (Cohen 1993, p344). Several studies have used this theory in an organizational context, where organizational structure is seen as promoting deviance in organizations (Mainemelis 2010; Warren 2003), but as yet, this theory has not been adopted by the IS community.

Organizational structure has been defined as rules or patterns of relationships, coordination, and communication existing within the organization between different work unit elements (individuals, groups, departments) (Blackburn 1982; Fredrickson 1988; Giddens 1979; Mintzberg 1983). It thus encompasses organizational policies, hierarchal levels, organizational goals and norms. Merton (1938), talking about social structure in general, suggests that structure exerts a "definite pressure" upon certain sections in a social system to engage in non-conforming behavior rather than conforming behavior. He presents two key elements of social structure as influencing deviance in social systems: firstly, the goals which the social system holds as legitimate (Mainemelis 2010) and secondly, the norms which define, control and regulate the acceptable modes or means of achieving those goals. According to Merton's Theory of Anomie, it is suggested that non-confirming or deviant behavior usually arises when a social system lacks appropriate capacity to provide certain individuals or groups within the system with access to legitimate means to achieve system prescribed goals. This condition is known as *Structural Strain* (Farnworth and and Leiber 1989; Guo et al. 2011; Mainemelis 2010; Merton 1938; Warren 2003). Mainemelis (2010), has used this concept in an organizational context, where he defines structural strain as a condition where the resources provided by an organization are insufficient to achieve the organizationally prescribed goals. He similarly argues that structural strain is responsible for generating deviance in organizations. Based on some of the existing studies on non-compliant IT behaviors, it is the view of the authors that feral IT practices in organizations are also driven by structural strain that arises when an organization fails to provide adequate resources to support organizationally prescribed goals. We thus see that Merton's theory of Anomie as appropriate for understanding the potential drivers that lead to feral IT practices.

Studies who have used Merton's theory in an organizational context suggest that the influence of organizational structure on structural strain is mediated by certain social influences. In this paper, we not only discuss the social influences but also the technological influences (see Figure 2 below) based on previous studies on deviant IT behaviors so as to understand how and why they lead to structural strain and ultimately promote feral practices in organizations. We suggest that both these influences (social and technological) produce or are produced by structural strain which has been shown to lead to deviant IT practices (see Figure 2 below). In Figure 2 we also suggest that apart from the technological and social influences which lead to structural strain, there are several supporting factors provided by the organizational structure, such as availability of relevant tools, technical skills etc which mediate the influence of structural strain on feral practices. This argument is based on the variation of Anomie theory proposed by Cloward (1959), who suggests that apart from certain social influences which promote conditions for deviance by generating structural strain, there are other supporting factors (arising from the structure of a society or organization) which mediate the influence of structural strain on deviance. In figure 2, we thus suggest that a mix of social and technological influences and supporting factors arising from the organizational structure, that give rise to feral practices.

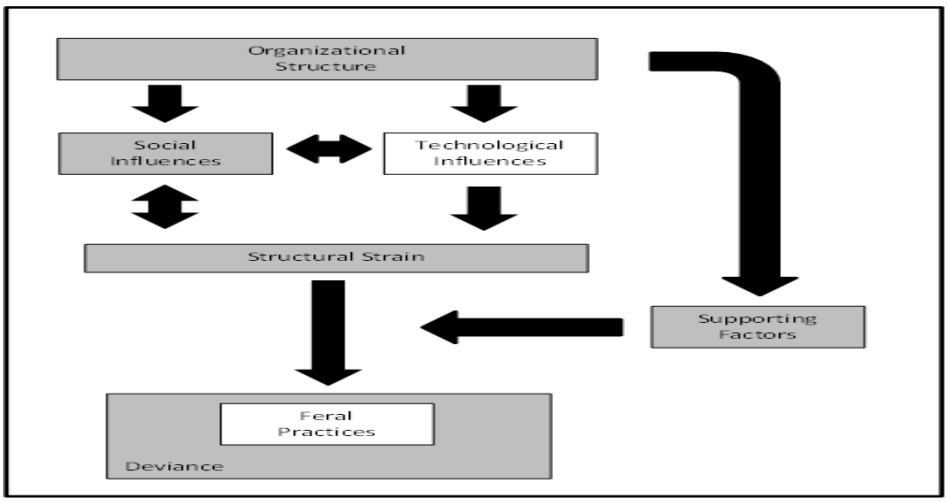

Figure 2: Structural Strain as a contributor to feral practices (Adapted from Merton (1938) & Cloward (1959))

Social Influence: Some of the potential contextual influences explored in previous research on non-compliant IT usage seem to have been (1) power and political struggles within the organization (Kerr et al. 2007; Markus

1983; Orlikowski 1991) (2) resistance to imposed organizational internal policies or procedures or technology (Azad and King 2008; Ferneley and Sobreperez 2006; Tyre and Orlikowski 1994) (3) lack of understanding regarding appropriate technology use due to absence of appropriate training or other appropriate learning avenues or skills (Boudreau and Robey 2005; Ferneley and Sobreperez 2006; Orlikowski 2000; Orlikowski and Gash 1994; Robey et al. 2002) and (4) influence from internal staff (peers, managers) (Leonardi 2007; Leonardi 2009).

Power has been defined as a capability of an individual or a group to achieve a required outcome or goal (Giddens 1979) whereas resistance is seen as an act of opposition possibly ensuing from perceived loss of power which arises when the individual or group is incapable of achieving its goal (Lapointe and Rivard 2005). Organizational structure which is defined as patterns or rules of interactions, coordination, and communication existing within the organization between different work unit elements (individuals, groups, departments) has been shown to delineate the distribution of power in organizations by providing organizational members access to resources to achieve their goals and also provide legitimacy required to use those resources (Markus 1983). Hence it could be argued that whenever structural strain arises for any reason (i.e. when organizations are incapable of providing its members access to legitimate resources to achieve legitimate goals), it could possibly lead to perceived loss of power that could lead to resistance. Hence power struggles and resistance may arise from structural strain. Previous studies have suggested that power and resistance act as potential contributors towards deviant IT practices in organizations. For instance in the study by Markus (1983), implementation of Financial Information System (FIS) was seen as leading to structural strain as divisional accountants lost control over their data and discretion to conduct tasks as per their requirements. This was ultimately perceived as a loss of power by divisional accountants who then engaged in the development of parallel systems or sabotaging the implemented FIS. Kerr et al. (2007) on the other hand provide an example of how an implemented SAP system was perceived as more of a financial system rather than for operational use. As the organization failed to provide the operational employees with the required technological resources to conduct their tasks, structural strain was seen to occur which was viewed as a loss of power by the operational staff who then engaged in feral practices.

Influence from intra-organizational entities or lack of understanding regarding appropriate technology usage can also be seen to produce structural strain. Organizational structure has been shown to influence the interactions between internal work unit elements. Also structure is seen to influence the distribution of the sources of information within the organization in the form of access to IT, training, advice etc (Leonardi 2007). Studies using these influences to account for deviance seem to suggest that influence from intra-organizational entities or lack of understanding lead to perception of technology as an impediment towards achievement of their goals (Leonardi 2009; Robey et al. 2002). Robey et al. (2002), in their study show that lack of familiarity with the ERP system and their further resistance to learn the system led the users to resort to spreadsheets to achieve their tasks. Leonardi (2009), on the other hand, highlighting the influence of intra-organizational influences, gives an example of how functionality offered by the official system was interpreted incorrectly due to interactions amongst employees which led to a perception of inadequacy of the system during its usage. This ultimately led to resistance to use of the technology.

Technological Influences: Organizations typically set specific expectations and norms (via internal policies and procedures, and the like) regarding the appropriate use of internal corporate IT resources. According to Orlikowski (1992), the organization's technology infrastructure, considered as a resource, not only embodies certain physical or material characteristics but also incorporates the structural properties (rules, norms, relationships) of the social system. The embedded structural properties not only enable users to perform certain tasks but also constrain some of them. When it is perceived that IT is not providing adequate means to achieve work related goals, deviance may be seen to occur. Studies by Behrens and Sedera (2004), Behrens (2009); Kerr and Houghton (2008); Kerr et al. (2007) and Leonardi (2011) seem to suggest that human actors, when confronted with technical limitations or constraints offered by the officially sanctioned systems, often resort to workarounds in order to achieve their intended goals. The technology constraints or limitations that have often been discussed are a perceived lack of functionality (Boudreau et al. 2005; Strong et al. 2010), inflexibility (Orlikowski 1992; Orlikowski 1996) and poor system quality (Azad and King 2011; Tyre and Orlikowski 1994; Volkoff et al. 2007). In order to address these constraints, users may either resort to alternative technologies or manipulate the current technology to achieve the desired ends outside the purview of the organizational norms. This has been illustrated by Behrens (2009), who gives an example of a web-based system (which was perceived by management as feral) that was developed to replace the current ERP system as it didn't offer the required functionality the users needed. Similarly Orlikowski (1991) provides an example of how consultants in a large software consulting firm manipulated the internal system in order to achieve the flexibility they needed to conduct their jobs.

While studies have shown how technological constraints lead to deviant behavior, it appears very few studies have analyzed the role of new technology capabilities leading to the same behavior. Switching to this perspective would enable us to understand how the capabilities of latest technologies would seem to facilitate structural strain. Consumerization of IT has put more technologies in the hands of the end users than ever before. This latest generation of technologies have been characterized by ease of use, easy availability and relatively low cost. At the same time users have grown more skilled in these technologies not only due to greater exposure but also due to easy availability of knowledge regarding the use of these technologies (Dearstyne 2007; King 2012). Because of this it could be said that users might be setting higher expectations with regards to the capabilities of the organization's existing technology infrastructure. When these organizations are seen as incapable or unwilling to provide the end-users with the desired capabilities, it could be said that structural strain might occur. End-users might thus resort to new technologies outside the purview of the organization's management in order to achieve their goals.

While we have tried to understand the social and the technological influences behind feral practices in isolation, we perceive that both these influences would have a bearing on each other. Studies do suggest that technology does have an influence on power relationships in organization and thus sometimes promotes resistance (Orlikowski 1992). On the other hand it is also suggested that the existing power relationships would influence how technology is designed, deployed and used in organization (Orlikowski 1992). This relationship is shown by the two-way arrow between the technological and social influences in Figure 2.

Mediation of supporting factors: While existing studies on feral practices seem to suggest structural strain as one of the pre-conditions for deviance, it could be added that apart from structural strain, another important influence might be the availability of relevant illegitimate opportunities/means to engage in deviant behavior. While structure does place constraints on the access to legitimate means, it similarly places constraints on the availability of illegitimate means as well, thus arguing that not every individual or a group would have equal access to the illegitimate opportunities to engage in deviant behavior (Cloward (1959); Cloward and Ohlin (1960); Merton (1959)). Thus the type of environment an individual or a group is situated in would influence the relative access to the illegitimate opportunities and thus would influence the nature of deviant behavior. In the context of feral practices, some of the supporting factors that might be suggested which could influence the availability to illegitimate opportunities/means could be the availability of relevant technological tools, technical skills, budget, support from the supervisors or local managers or peers, availability of time, and existing compliance structures (Lehman and Ramanujam 2009) to monitor feral initiatives and enforce organizational level norms etc. It could be added that consumerization of IT could be providing further opportunities to end users to engage in feral practices as relevant tools to engage in these behaviors are relatively easily accessible and convenient to use.

Looking at the current studies on feral systems, it appears that there is a great deal of focus on uncovering the technological and social influences behind deviance, but considerably less focus on understanding what supporting factors give rise to this behavior. Furthermore the concept of structural strain, though evident in the examples provided by the existing studies, has not been explicitly discussed as the potential cause for deviant IT practices. This model thus provides a comprehensive picture about feral practices by explaining why feral practices emerge, what technological and social factors might promote these practices and also identifying what supporting factors might be responsible for generating this behavior. We currently see no studies which have taken this comprehensive approach in accounting for non-compliant IT behaviors associated with feral practices.

CONCLUSION

We see that our paper makes three important contributions in IS research. Firstly we argue that taking a practice perspective, where the focus is more on the usage of IT systems enables us to develop a greater understanding of the phenomenon. Orlikowski (2000) similarly advocates the focus on usage by suggesting that researchers and managers assessing the performance impact of technological investment would get better results when they place a greater emphasis on understanding how technology is being used in the day-to-day activities of the end-users. She adds that 'whether and how people interact' with technology in their work activities and 'not the mere presence' of technology, influences the performance outcomes and consequences of IT (Orlikowski 2000, p425). Furthermore a practice perspective not only allows us to focus on usage but also explore the perceptions of the end-users who engage in those behaviors and also account for the social contextual influences behind them. We thus see that taking a practices perspective would provide a holistic view of the phenomenon.

We further see that taking a practices perspective opens the door to considering a whole range of feral initiatives of the end-users which not only includes use of systems which reside outside the corporate IT infrastructure, but also includes the ones which are a part of the organization's infrastructure but used in a feral ways by the end-users. This also opens the possibility to incorporate the concept of non-usage (which includes behaviors where

the users avoid the use of corporate systems altogether resorting to alternative means) or delegated usage (which includes design of smart systems where there is minimum human intervention required). While not explored in this study, we see that understanding different patterns of IT usage would open researchers to new range of feral practices.

We ultimately see that taking a practice perspective makes more logical sense taking into consideration the current organizational IT landscape. Recent trends of BYOD (Bring Your Own Device) or Consumerization of IT have blurred the lines between the official and unofficial systems. With IT becoming more pervasive, user friendly and easy to use, users now seem to have greater accessibility and knowledge on IT. Statistics provided by Gartner and PwC seem to suggest that end users have a greater sense than the corporate IT department of what products and services are suitable to their needs and thus seem have greater control on IT spending than the corporate IT department (King 2012). But at the same time, the IT department still holds the responsibility for ensuring that the end-users use IT in a manner which doesn't jeopardize the organizations interests. Hence the focus seems to be not just on what IT systems the users use but also on the usage of IT systems as per the organizations standards and policies.

Secondly, by outlining the scope of feral practices, we suggest that feral practices are not all bad news for an organization. We argue that while some feral practices are potentially risky and may be of concern to an organization, there are others which might be potentially beneficial and may act as a source of innovation. Hence organizations need to understand how to maintain a balance of policies which on one hand discourages end-users from engaging in the potentially risky IT practices and at the same time encourages innovative and potentially beneficial practices which could add value to the organization. Currently very few studies have attempted to highlight the innovative and beneficial aspects of feral practices and hence there is need of a greater research which explores the ways in which these practices could add value to an organization.

Finally this study provides a comprehensive model which not only explains why feral practices come about but also highlights some of the social, technological and supporting influences which promote this behavior. We see this model being useful in understanding feral practices of end users in organizations. This model actually draws on Merton's theory of Anomie which has been extensively used to understand deviance in societies as well as organizations. The theory's extensive application in the organizational deviance literature makes it suitable for understanding feral practices where the focus is on the deviant IT behaviors of the end users. Currently we see no studies on feral practices offering a coherent view of why feral practices come about and what influences drive them. As this study draws from previous studies on non-compliant IT behaviors, the model that we have developed incorporates all the different views offered by the studies under a single model and thus provides a holistic view of these practices.

REFERENCES

Azad, B., and King, N. "Enacting computer workaround practices within a medication dispensing system," *European Journal of Information Systems* (17) 2008, p 15.

Azad, B., and King, N. "Institutionalized computer workaround practices in a Mediterranean country: an examination of two organizations," *European Journal of Information Systems*) 2011, p 15.

Behrens, S. "Shadow systems: the good, the bad and the ugly," *Communications of the ACM* (52:2) 2009, p 6.

Behrens, S., and Sedera, W. "Why Do Shadow Systems Exist after an ERP Implementation? Lessons from a Case Study," *Association for Information Systems*) 2004, p 15.

Blackburn, R. S. "Dimensions of Structure: A Review and Reappraisal," *Academy of Management Review* (7:1) 1982, p 8.

Boudreau, M.-C., and Robey, D. "Enacting Integrated Information Technology: A Human Agency Perspective," *Organization Science* (16:1) 2005, p 16.

Cloward, R. A. "Illegitimate Means, Anomie, and Deviant Behavior," *American Sociological Review* (24:2) 1959, p 13.

Cloward, R. A., and Ohlin, L. E. "Delinquency and Opportunity," in: *Criminology Theory: Selected Classical Readings*, G. Eccleston (ed.), Anderson Publishing Co., Cincinnati, OH 1960.

Cohen, D. V. "Creating and Maintaining Ethical Work Climates: Anomie in the Workplace and Implications for Managing Change," *Business Ethics Quarterly* (3:4) 1993, p 16.

Damanpour, F. "Organizational Innovation: A Meta-Analysis of Effects of Determinants and Moderators," *Academy of Management Journal* (34:3) 1991, p 36.

Dearstyne, B. W. "Blogs, Mashups, & Wikis Oh, My!," *Information Management Journal* (41:4) 2007, p 8.

Downs, G. W., and Mohr, L. B. "Conceptual Issues in the Study of Innovation," *Administrative Science Quarterly* (21:4) 1976, p 15.

Downs, G. W., and Mohr, L. B. "Toward a Theory of Innovation," *Administration and Society* (10:4) 1979, p 30.
Dubin, R. "Deviant Behavior and Social Structure: Continuities in Social Theory," *American Sociological Review* (24:2) 1959, p 18.
Farnworth, M., and Leiber, M. J. "Strain Theory Revisited: Economic Goals, Educational Means, and Delinquency," *American Sociological Review* (54:2) 1989, p 12.
Ferneley, E. H., and Sobreperez, P. "Resist, comply or workaround? An examination of different facets of user engagement with information systems," *European Journal of Information Systems* (15) 2006, p 12.
Finnegan, P., and Longaigh, S. N. "Examining the effects of information technology on control and coordination relationships: an exploratory study in subsidiaries of pan-national corporations," *Journal of Information Technology* (17:3) 2002, p 15.
Fredrickson, J. W. "The Strategic Decision Process and Organizational Structure," *Academy of Management Review* (11:2) 1988, p 18.
Giddens, A. *Central Problems in Social Theory: Action, Structure and Contradiction in Social Analysis* The Macmillan Press Ltd, London and Basingstoke, 1979.
Guo, K. H., Yuan, Y., Archer, N. P., and Connelly, C. E. "Understanding Nonmalicious Security Violations in the Workplace: A Composite Behavior Model," *Journal of Management Information Systems* (28:2) 2011, p 34.
Kerr, D., and Houghton, L. "Feral Systems: The Likely Effects on Business Analytics Functions in an Enterprise Resource Planning System Environment," *Association for Information Systems*) 2008.
Kerr, D. V., Houghton, L., and Burgess, K. "Power Relationships that lead to the Development of Feral Systems," *Australasian Journal of Information Systems* (14:2) 2007, p 12.
King, J. "The Upside of Shadow IT," www.computerworld.com, 2012.
Kobayashi, M., Fussell, S. R., Xiao, Y., and Seagull, F. J. "Work Coordination, Workflow, and Workarounds in a Medical Context," CHI EA '05 CHI '05 extended abstracts on Human factors in computing systems, ACM, Portland, Oregon, USA, 2005.
Koopman, P., and Hoffman, R. R. "Work-arounds, Make-work, and Kludges," *Human Centered Computing* (18:6) 2003, p 6.
Lapointe, L., and Rivard, S. "A Multilevel Model of Resistance to Information Technology Implementation," *MIS Quarterly* (29:3) 2005, p 31.
Lehman, D. W., and Ramanujam, R. "Selectivity in Organizational Rule Violations," *Academy of Management Review* (34:4) 2009, p 15.
Leonardi, P. M. "Activating the Informational Capabilities of Information Technology for Organizational Change," *Organization Science* (18:5) 2007, p 29.
Leonardi, P. M. "Why Do People Reject New Technologies and Stymie Organizational Changes of Which They Are in Favor? Exploring Misalignments Between Social Interactions and Materiality," *Human Communication Research* (35:3) 2009, p 35.
Leonardi, P. M. "When Flexible Routines Meet Flexible Technologies: Affordance, Constraint, and the Imbrication of Human and Material Agencies," *MIS Quarterly* (35:1) 2011, p 21.
Mainemelis, C. "Stealing Fire: Creative Deviance in the Evolution of New Ideas," *Academy of Management Review* (35:4) 2010, p 21.
Markus, L. M. "Power, Politics, and MIS Implementation," *Communications of the ACM* (26:6) 1983, p 15.
Merton, R. K. "Social Structure and Anomie," *American Sociological Review* (3:5) 1938, p 11.
Merton, R. K. "Social Conformity, Deviation, and Opportunity Structures: A Comment on the Contributions of Dubin and Cloward," *American Sociological Review* (24:2) 1959, p 13.
Mintzberg, H. *Structure in Fives* Prentice Hall Inc. , Engelwood Cliffs, New Jersey 1983.
Orlikowski, W. J. "Integrated information environment or matrix of control? The contradictory implications of information technology," *Accounting, Management and Information Technologies* (1:1) 1991, p 34.
Orlikowski, W. J. "The Duality of Technology: Rethinking the Concept of Technology in Organizations," *Organization Science* (3:3) 1992, p 30.
Orlikowski, W. J. "Improvising Organizational Transformation Over Time: A Situated Change Perspective," *Information Systems Research* (7:1) 1996, p 30.
Orlikowski, W. J. "Using Technology and Constituting Structures : A Practice Lens for Studying Technology in Organizations," *Organization Science* (11:4) 2000, p 25.
Orlikowski, W. J., and Gash, D. C. "Technological frames: making sense of information technology in organizations," *ACM Transactions on Information Systems* (12:2) 1994, p 34.
Reckwitz, A. "Toward a Theory of Social Practices : A Development in Culturalist Theorizing," *European Journal of Social Theory* (5:2) 2002, p 21.

Robey, D., Ross, J. W., and Boudreau, M.-C. "Learning to Implement Enterprise Systems: An Exploratory Study of the Dialectics of Change," *Journal of Management Information Systems* (19:1) 2002, p 30.
Schatzki, T. R. "Introduction : Practice theory," in: *Practice Turn in Contemporary Theory*, T.R. Schatzki, K. Knorr-Cetina and E. Savigny (eds.), Routledge, Florence, KY, USA 2000.
Slappendel, C. "Perspectives on Innovation in Organization," *Organization Studies* (17:1) 1996, p 23.
Strong, D. M., and Volkoff, O. "Understanding Organization-Enterprise System Fit: A Path To Theorizing The Information Technology Artifact," *MIS Quarterly* (34:4) 2010, p 26.
Tyre, M. J., and Orlikowski, W. J. "Windows of Opportunity: Temporal Patterns of Technological Adaptation in Organizations," *Organization Science* (5:1) 1994, p 21.
Volkoff, O., Strong, D., and Elmes, M. "Technological Embeddedness and Organizational Change," *Organization Science* (18:5) 2007, p 17.
Warren, D. E. "Constructive and Destructive Deviance In Organizations," *Academy of Management Review* (28:4) 2003, p 11.

COPYRIGHT